PAT-NO: JP411085881A

DOCUMENT-IDENTIFIER: JP 11085881 A

TITLE: METHOD AND SYSTEM FOR ELECTRONIC TRANSFER

PUBN-DATE: March 30, 1999

INVENTOR-INFORMATION:

NAME	COUNTRY
HASHIZUME, HIROYUKI	

ASSIGNEE-INFORMATION:

NAME	COUNTRY
TOSHIBA CORP	N/A

APPL-NO: JP09243017

APPL-DATE: September 8, 1997

INT-CL (IPC): G06F019/00

ABSTRACT:

PROBLEM TO BE SOLVED: To eliminate an unauthorized transfer request, except from a transfer requester and also to insure security by notifying beforehand an encipher key for transfer data from a financial institution side to a transfer requester, based on an application from the transfer requester.

SOLUTION: An electronic transfer terminal 20 enciphers transfer data by an encipher key for transfer data and transmits the enciphered transfer data to an electronic transfer controller 30 on a financial institution side via a communication network 40, when a transfer requester inputs the transfer data with the encipher key for transfer data, that is acquired through advance examination on the financial institution side registered on an encipher key registering part 23 for transfer data. After that, when a decoding key for is transmitted from the controller 30, it is taken in and registered on a decoding key registering part 26 for verification. Next, when enciphered transfer data and a check result are transmitted from the financial institution side, the transfer data and check result are decoded by using the registered decoding key for verification.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－85881

(43)公開日　平成11年(1999)３月30日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　19/00		Ｇ０６Ｆ　15/30	３６０
			３５０

審査請求　未請求　請求項の数３　ＯＬ　（全９頁）

(21)出願番号　特願平9－243017

(22)出願日　平成９年(1997)９月８日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　橘詰　弘之
東京都府中市東芝町１番地　株式会社東芝府中工場内

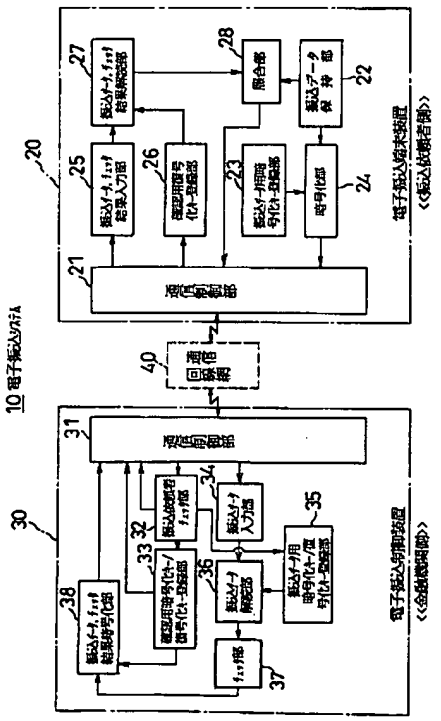
(74)代理人　弁理士　三好　秀和　（外３名）

(54)【発明の名称】　電子振込方法及び電子振込システム

(57)【要約】

【課題】　通信回線を介して、振込の依頼を行う際、事前に申し込んだ振込依頼者以外からの不正な振込依頼を無くし、これによってセキュリティを確保するとともに、振込依頼者以外の第３者に振込内容が知られないようにして、プライバシーを確保する。

【解決手段】　申込者からの申込が事前にあったとき、申込者の審査を行い、振込を許可するとき、振込データ用暗号化キーを通知し、申込者から前記振込データ用暗号化キーで暗号化された振込データが送信されてきたとき、確認用復号化キーを申込者に送信するとともに、前記確認用復号化キーに対応する確認用暗号化キーを使用して、前記振込データを暗号化して、前記申込者に送信し、振込データの内容を確認させる。



1

【特許請求の範囲】

【請求項１】　振込依頼者からの申込に基づき、金融機関側から前記振込依頼者に振込データ用暗号化キーを事前に通知し、

金融機関側では、前記振込依頼者から前記振込データ用暗号化キーを使用して暗号化した振込手続きがあったときには、前記振込データ用暗号化キーに対応する振込データ用復号化キーを使用して前記振込手続きを復元し、この振込手続きが正規のものであるときには、金融機関側から前記振込依頼者に確認用復号化キーを通知するとともに、この確認用復号化キーに対応する確認用暗号化キーを使用して、振込確認内容を暗号化して、前記振込依頼者に戻し、

振込依頼者側では、通知された確認用復号化キーを使用して、前記振込確認内容を復号化するとともに、その内容を確認して、前記金融機関側に振込指示通知を出し、この振込依頼通知を受け取ったときに、金融機関側では、依頼された振込処理を行うこと、

を特徴とする電子振込方法。

【請求項２】　振込依頼者からの申込に基づき、金融機関側から前記振込依頼者に振込データ用暗号化キーを事前に通知するとととともに、ＩＣカードが渡され、

振込依頼者側では、事前通知された前記振込データ用暗号化キーを使用して暗号化された振込データを前記ＩＣカードに記憶させて、金融機関側に提出し、

金融機関側では、このＩＣカードが提出された場合には、振込依頼者側に照会番号を通知するとともに、前記振込データ用暗号化キーに対応する振込データ用復号化キーを使用して、ＩＣカードに記憶されている暗号化された振込データを復号し、復号された振込データの内容に基づき、振込を許可するかどうかを判定し、次いで、振込依頼者側から前記照会番号が通知され、かつこの照会番号が正規の照会番号であると判定した場合には、振込依頼者に前記判定結果を通知し、

前記振込依頼者側では、この通知内容に基づいて、金融機関側に振込指示通知、または振込キャンセル通知を行うこと、

特徴とする電子振込方法。

【請求項３】　振込依頼者側に設けられた電子振込端末装置と、金融機関側に設けられた電子振込制御装置とを通信回線網により相互に接続し、電子振込端末装置からの振込手続を受けた電子振込制御装置により振込処理を実行する電子振込システムであって、

前記電子振込端末装置は、

予め通知されている振込データ用暗号化キーにより振込データを暗号化して前記電子振込制御装置に送信する手段と、

振込確認のために前記電子振込制御装置から供給されてきた振込データ及びチェック結果を入力する手段と、

前記電子振込制御装置から通知された確認用復号化キー

2

を使用して、入力された振込データ及びチェック結果を復号する手段と、

復号された振込データと前記送信済みの振込データとを照合する手段と、

両データの照合一致が確認された場合に限り、前記電子振込制御装置に振込指示通知を出力する手段とを備え、

前記電子振込制御装置は、

前記電子振込端末装置から暗号化された振込データが供給された場合に、前記振込データ用暗号化キーに対応する振込データ用復号化キーを使用して前記振込データを復号する手段と、

復号の結果、この振込データが正規のものである場合には、前記振込依頼者に確認用復号化キーを通知する手段と、

この確認用復号化キーに対応する確認用暗号化キーを使用して、前記復号された振込データ及びチェック結果を暗号化するとともに、この暗号化された振込データ及びチェック結果を前記電子振込端末装置に送信する手段と、

この振込データ及びチェック結果に応答した前記電子振込端末装置からの前記振込指示通知を受信した場合には、依頼された振込処理を実行する手段と、

を備えたことを特徴とする電子振込システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、振込手続きを行う際、振込依頼者のプライバシーを保護し、セキュリティを確保する電子振込方法及び電子振込システムに関する。

【０００２】

【従来の技術】現在、金融機関に振込依頼を行うときには、振込先や、振込金額などを書き込んだ振込依頼書を金融機関側に持ち込んで窓口に提出し、金融機関側で所定事項をチェックした後に振込を実行可能にしている。

【０００３】

【発明が解決しようとする課題】しかしながら、上述した従来の振込手順においては、次に述べるような問題があった。

【０００４】まず、振込先、振込金額などを書き込んだ振込依頼書を金融機関側に持ち込んで、これを窓口などに提出するようにしているので、振込依頼書を窓口に提出する際に振込依頼書の内容が第３者の目に触れると、その内容が知られ、プライバシーが漏れてしまうという恐れがあった。

【０００５】そこで、電話回線を使用し、会社内などのコンピュータ装置を操作して、金融機関側に振込依頼を行う方法も検討されているが、振込内容をそのまま金融機関に伝送した場合には、電話回線上で振込内容が第３者に漏れてしまう危険性があり、セキュリティを確保することが難しい。

【０００６】また、第３者が本来の振込依頼者に成り済まして、金融機関側に偽の振込依頼を出した場合などに至っては、金融機関側では、間違った振込処理を行ってしまう恐れがあった。

【０００７】本発明は上記の事情に鑑み、請求項１、３では、通信回線を介して、振込の依頼を行う際、事前に申し込んだ振込依頼者以外からの不正な振込依頼を無くすことができ、これによってセキュリティを確保することができるとともに、振込依頼者以外の第３者に振込内容が知られないようにして、プライバシーを確保することができる電子振込方法及び電子振込システムを提供することを目的としている。

【０００８】また、請求項２では、ＩＣカードを使用して、振込の依頼を行う際、事前に申し込んだ振込依頼者以外からの不正な振込依頼を無くすことができ、これによってセキュリティを確保することができるとともに、振込依頼者以外の第３者に振込内容が知られないようにして、プライバシーを確保することができる電子振込システムを提供することを目的としている。

【０００９】

【課題を解決するための手段】上記の目的を達成するために本発明は、請求項１では、振込依頼者からの申込に基づき、金融機関側から前記振込依頼者に振込データ用暗号化キーを事前に通知し、金融機関側では、前記振込依頼者から前記振込データ用暗号化キーを使用して暗号化した振込手続きがあったときには、前記振込データ用暗号化キーに対応する振込データ用復号化キーを使用して前記振込手続きを復元し、この振込手続きが正規のものであるときには、金融機関側から前記振込依頼者に確認用復号化キーを通知するとともに、この確認用復号化キーに対応する確認用暗号化キーを使用して、振込確認内容を暗号化して、前記振込依頼者に戻し、振込依頼者側では、通知された確認用復号化キーを使用して、前記振込確認内容を復号化するとともに、その内容を確認して、前記金融機関側に振込指示通知を出し、この振込依頼通知を受け取ったときに、金融機関側では、依頼された振込処理を行うことを特徴としている。

【００１０】また、請求項２では、振込依頼者からの申込に基づき、金融機関側から前記振込依頼者に振込データ用暗号化キーを事前に通知するとととともに、ＩＣカードが渡され、振込依頼者側では、事前通知された前記振込データ用暗号化キーを使用して暗号化された振込データを前記ＩＣカードに記憶させて、金融機関側に提出し、金融機関側では、このＩＣカードが提出された場合には、振込依頼者側に照会番号を通知するとともに、前記振込データ用暗号化キーに対応する振込データ用復号化キーを使用して、ＩＣカードに記憶されている暗号化された振込データを復号し、復号された振込データの内容に基づき、振込を許可するかどうかを判定し、次いで、振込依頼者側から前記照会番号が通知され、かつこ

の照会番号が正規の照会番号であると判定した場合には、振込依頼者に前記判定結果を通知し、前記振込依頼者側では、この通知内容に基づいて、金融機関側に振込指示通知、または振込キャンセル通知を行うこと特徴としている。

【００１１】さらに、請求項３では、振込依頼者側に設けられた電子振込端末装置と、金融機関側に設けられた電子振込制御装置とを通信回線網により相互に接続し、電子振込端末装置からの振込手続を受けた電子振込制御装置により振込処理を実行する電子振込システムであって、前記電子振込端末装置は、予め通知されている振込データ用暗号化キーにより振込データを暗号化して前記電子振込制御装置に送信する手段と、振込確認のために前記電子振込制御装置から供給されてきた振込データ及びチェック結果を入力する手段と、前記電子振込制御装置から通知された確認用復号化キーを使用して、入力された振込データ及びチェック結果を復号する手段と、復号された振込データと前記送信済みの振込データとを照合する手段と、両データの照合一致が確認された場合に限り、前記電子振込制御装置に振込指示通知を出力する手段とを備え、前記電子振込制御装置は、前記電子振込端末装置から暗号化された振込データが供給された場合に、前記振込データ用暗号化キーに対応する振込データ用復号化キーを使用して前記振込データを復号する手段と、復号の結果、この振込データが正規のものである場合には、前記振込依頼者に確認用復号化キーを通知する手段と、この確認用復号化キーに対応する確認用暗号化キーを使用して、前記復号された振込データ及びチェック結果を暗号化するとともに、この暗号化された振込データ及びチェック結果を前記電子振込端末装置に送信する手段と、この振込データ及びチェック結果に応答した前記電子振込端末装置からの前記振込指示通知を受信した場合には、依頼された振込処理を実行する手段とを備えたことを特徴としている。

【００１２】上記の構成において、請求項１、３では、振込依頼者からの申込に基づき、金融機関側から振込依頼者に振込データ用暗号化キーを事前に通知する。振込依頼者から振込データ用暗号化キーを使用して暗号化した振込手続きがあったときには、金融機関側では、振込データ用暗号化キーに対応する振込データ用復号化キーを使用して振込手続きを復元する。この振込手続きが正規のものであれば、金融機関側では振込依頼者に確認用復号化キーを通知した後、この確認用復号化キーに対応する確認用暗号化キーを使用して振込確認内容を暗号化し、振込依頼者に戻す。振込依頼者側では、確認用復号化キーを使用して振込確認内容を復号化し、内容を確認する。そして、金融機関側に振込指示通知を出したときに、金融機関側では、依頼された振込処理を実行する。このため、通信回線を介して振込の依頼を行う際、事前に申し込んだ振込依頼者以外からの不正な振込依頼を無

くし、これによってセキュリティを確保するとともに、振込依頼者以外の第３者に振込内容が知られないようにして、プライバシーを確保する。

【００１３】また、請求項２では、振込依頼者と、金融機関との間で、暗号化キーと、ＩＣカードとを使用して電子振込手続きを行うことにより、ＩＣカードを使用して、振込の依頼を行う際、事前に申し込んだ振込依頼者以外からの不正な振込依頼を無くし、これによってセキュリティを確保するとともに、振込依頼者以外の第３者に振込内容が知られないようにして、プライバシーを確保する。

【００１４】

【発明の実施の形態】

《第１の実施の形態の構成》図１は本発明に係る電子振込システムの実施の形態を示すブロック図である。

【００１５】この図に示す電子振込システム１０は、振込依頼者側に設けられたパーソナルコンピュータなどで構成される電子振込端末装置２０と、金融機関に設けられたコンピュータ等で構成される電子振込制御装置３０と、電子振込端末装置２０と電子振込制御装置３０とを相互に接続する通信回線網４０とを備えており、振込依頼者から振込依頼があったとき、電子振込端末装置２０と、電子振込制御装置３０との間で、振込データ用暗号化キー、確認用復号化キーを使用した暗号通信を行って、金融機関側に振込処理を行わせるように構成されている。

【００１６】この場合、電子振込端末装置２０は、通信回線網４０を介して電子振込制御装置３０との間でデータの送受信を実行する通信制御部２１と、振込依頼者が作成した振込データを入力して一時保持する振込データ保持部２２と、金融機関側から振込依頼者に通知された振込データ暗号化キーを登録保持する振込データ用暗号化キー登録部２３と、この登録された振込データ用暗号化キーを使用して振込データ保持部２２に一時記憶されている振込データを暗号化する暗号化部２４と、電子振込制御装置３０から供給されてきた振込データ、チェック結果を入力する振込データ、チェック結果入力部２５と、電子振込制御装置３０から通知された確認用復号化キーを登録保持する確認用復号化キー登録部２６と、この確認用復号化キーを使用して入力された振込データ、及びチェック結果を解読する振込データ、チェック結果解読部２７と、解読された振込データと振込データ保持部２２に保持されている振込データとを照合する照合部２８とを備えている。なお、当該電子振込端末装置と振込依頼者との間のマンマシンインタフェースとなるディスプレイ装置や、キーボードなどの図示は省略されている。

【００１７】この電子振込端末装置２０では、金融機関側の事前審査で得られた振込データ用暗号化キーが振込データ用暗号化キー登録部２３に登録されている状態で、振込依頼者によってキーボードから振込データが入力されたとき、振込データ用暗号化キーによって前記振込データを暗号化し、通信回線網４０を介して、暗号化された振込データを金融機関側の電子振込制御装置３０に伝送する。その後、この電子振込制御装置３０から確認用復号化キーが伝送されてきたとき、これを取り込んで確認用復号化キー登録部２６に登録する。次いで、金融機関側から暗号化された振込データ、チェック結果が伝送されてきたとき、登録されている確認用復号化キーを使用して、前記振込データ、チェック結果を復号する。そして、照合部２８では、振込依頼の内容を振込依頼者に確認させるとともに、照合部２８では、送信データを受信データとの照合一致を確認し、その確認内容を金融機関側に伝送する。

【００１８】また、電子振込制御装置３０は、通信回線網４０を介して電子振込端末装置２０との間でデータの送受信を実行する通信制御部３１と、振込依頼者が正当であるか否かをチェックする振込依頼者チェック部３２と、確認用暗号化キー及びこれに対応する振込依頼者側に通知される確認用復号化キーを登録保持する確認用暗号化キー／復号化キー登録部３３と、電子振込端末装置２０から暗号化された振込データが供給された場合にこれを入力する振込データ入力部３４と、振込依頼者に事前通知された前記振込データ暗号化キーとそれに対応する復号化キーとを登録保持する振込データ用暗号化／復号化キー登録部３５と、この復号化キーを使用して入力された振込データを解読する振込データ解読部３６と、解読された振込データの内容をチェックするチェック部３７と、解読された振込データおよびそのチェック結果を前記確認用暗号化キーを使用して暗号化する振込データ、チェック結果暗号化部３８とを備えている。なお、ここでも当該電子振込制御装置と金融機関側オペレータとの間のマンマシンインタフェースとなるディスプレイ装置や、キーボードなどの図示は省略されている。

【００１９】この電子振込制御装置３０では、通信回線網４０を介して、電子振込端末装置２０から接続要求があったとき、回線接続元番号（発呼元の電話番号）をチェックして、事前審査で振込許可が出されている正規の振込依頼者かどうかをチェックし、正規の振込依頼者からの接続要求であれば、電子振込端末装置２０から暗号化された振込データが伝送されてきたとき、確認用復号化キーを電子振込端末装置２０に伝送する。この後、振込データ用暗号化キーに対応する振込データ用復号化キーを使用して、前記振込データを復号化してオペレータに提示し、これをチェックさせた後、前記確認用復号化キーに対応する確認用暗号化キーを使用して、前記振込データ、チェック結果を暗号化して、電子振込端末装置２０に伝送する。そして、電子振込端末装置２０から確認内容が伝送されてきたとき、この確認内容に応じた振込処理やキャンセル処理などを行う。

【００２０】《第１の実施の形態の動作》次に、図２～図６に示すフローチャートを参照しながら、この実施の形態の動作を説明する。

【００２１】＜事前審査手続き＞まず、図２のフローチャートに示すように、電子振込端末装置２０を使用した振込依頼手続きに先だち、振込依頼者によって、会社名や会社側の電子振込端末装置２０が接続された電話の番号など、必要な事項が記載された申込書が作成され、これが金融機関側の窓口に提出される（ステップＳＴ１）。

【００２２】これに応答して金融機関側では、前記申込書の内容に基づき、申込者の取引実績や資産などを加味して、申込者に通信回線網４０経由での振込を許可するかどうかが審査される。振込を許可しない場合には、不許可通知書が作成されて、これが申込者に通知される（ステップＳＴ２）。一方、振込を許可する場合には、申込者毎に固有の「振込データ用暗号化キー」が決定され、これが申込者に通知される（ステップＳＴ３）。

【００２３】この場合、振込データ用暗号化キーは、暗号化された振込データが通信回線網４０経由で送信されてきたときに、この振込データが申込者（正規の振込依頼者）からの振込データかどうかを識別するために使用される。

【００２４】この申込者に対して、金融機関側からの前述したような振込許可が通知されている場合には、この申込者は、電子振込端末装置２０のキーボードを操作して、金融機関側から通知された振込データ用暗号化キーを振込データ用暗号化キー登録部２３に登録する。

【００２５】＜振込依頼手続き＞この後、図３のフローチャートに示すように、前記申込者と同一または関係する振込依頼者によって電子振込端末装置２０が操作されて、振込データが作成されると（ステップＳＴ５）、これが振込データ保持部２２に一時保存される。次いで、暗号化部２４では、既に登録されている振込データ用暗号化キーによって振込データが暗号化されて一時記憶される（ステップＳＴ６）。そして、通信回線網４０を介して電子振込制御装置３０に電話がかけられる（ステップＳＴ７）。

【００２６】電子振込制御装置３０側では、通信回線網４０を介して電話が受けられると、通信回線網４０から通知される発呼元の電話番号が、既に振込許可を出している振込依頼者（振込データ用暗号化キーを通知してある申込者）側の電話番号かどうかが振込依頼者チェック部３２によりチェックされる。発呼元の電話番号が既に振込許可を出している振込依頼者側の電話番号でなければ、不正なアクセスであると判断されて、即座に通信回線が切断される（ステップＳＴ８、ＳＴ９）。

【００２７】また、発呼元の電話番号が既に振込許可を出している振込依頼者側の電話番号であれば、電子振込制御装置３０によって発呼元の電子振込端末装置２０との間の通信回線が確立されるとともに、送信許可応答が生成され、これが通信回線網４０を介して、電子振込端末装置２０に送信される（ステップＳＴ８）。

【００２８】そして、図４のフローチャートに示すように、振込依頼者側の電子振込端末装置２０によって、送信許可応答が受信されると、既に作成されて、一時記憶されている暗号化された振込データが通信回線網４０を介して金融機関側の電子振込制御装置３０に送信される。

【００２９】電子振込端末装置２０から送信される暗号化された振込データが振込データ入力部３４に入力されると（ステップＳＴ１０）、発呼元（申込者）毎に固有の「確認用復号化キー」が決定され、これが振込依頼者側の電子振込端末装置２０に通知された後（ステップＳＴ１１）、通信回線が切断される（ステップＳＴ１２）。

【００３０】＜振込依頼確認手続き＞この後、図５のフローチャートに示すように、金融機関側の電子振込制御装置３０では、振込データ用暗号化キー／復号化キー登録部３５に登録されている、前記発呼元の電話番号に割り振った振込データ用暗号化キーに対応する振込データ用復号化キーが使用されて、前記振込データが復号化される（ステップＳＴ１５、ＳＴ１６）。これが正常に復号化できたとき、申込者しか知らない振込データ用暗号化キーを使用した正規の振込データであると判定されるとともに、復号化された振込データがオペレータに提示されるとともに、チェック部３７により前記振込データで示される振込先金融機関が存在するかどうか、振込金額の合計が妥当な金額かどうかなどがチェックされる（ステップＳＴ１７）。

【００３１】次いで、前記振込データの内容が正しい振込内容であると確認されると、振込データ、チェック結果暗号化部３８では、確認用暗号化キー／復号化キー登録部３３に登録されている前記確認用復号化キーに対応する確認用暗号化キーを使用して、前記振込データ、前記チェック結果が暗号化される（ステップＳＴ１８、ＳＴ１９）。そして、通信回線網４０を介して、前記振込依頼者側の電子振込端末装置２０に電話がかけられ、暗号化された振込データ（受信データ）、チェック結果が振込依頼者側の電子振込端末装置２０に送信される（ステップＳＴ２０）。

【００３２】図６のフローチャートに示すように、電子振込制御装置３０から送信される暗号化された振込データ、チェック結果が振込データ、チェック結果入力部２４で入力されると（ステップＳＴ２１）、振込データ、チェック結果解読部２７では、確認用復号化キー登録部２６に登録されている確認用復号化キー（振込データを金融機関側に送信した者しか知らない復号化キー）を使用して、前記振込データ、チェック結果を復号化する。復号化された振込データ、チェック結果は振込依頼者に

提示される（ステップＳＴ２２）。

【００３３】この後、照合部２８では、金融機関側から送信されてきた振込データの内容、チェック結果の内容と、金融機関側に依頼した振込データの内容とが突き合わせチェックされ、自分が送信した振込データの内容と、金融機関側から送信されてきた振込データの内容とが異なっているときその旨を通知する。チェックの結果、送信した振込データと相違する場合には（ステップＳＴ２３）、振込データなどにエラーがあったと判定されて、この判定結果に基づき、振込キャンセル通知が作成され、これが金融機関側の電子振込制御装置３０に送信されて、振込処理がキャンセルされた後、通信回線が切断される（ステップＳＴ２４、ＳＴ２５）。

【００３４】また、自分が送信した振込データの内容と、金融機関側から送信されてきた振込データの内容とが合致し、チェック結果が満足するものであるときには（ステップＳＴ２３）、振込データの送信が正しく行われたと判定され、この判定結果に基づき、電子振込端末装置２０が操作されて、振込指示通知が作成され、これが金融機関側の電子振込制御装置３０に送信されて、振込処理が実施された後、通信回線が切断される（ステップＳＴ２６、ＳＴ２７）。

【００３５】《第１の実施の形態の効果》このようにこの実施の形態においては、申込者からの申込が事前にあったとき、申込者の審査を行い、振込を許可するとき、振込データ用暗号化キーを通知し、申込者から前記振込データ用暗号化キーで暗号化された振込データが送信されてきたとき、確認用復号化キーを申込者に送信するとともに、前記確認用復号化キーに対応する確認用暗号化キーを使用して、前記振込データを暗号化して、前記申込者に送信し、振込データの内容を確認させるようにした。このため、通信回線網４０を介して、振込の依頼を行う際、事前に申し込んだ振込依頼者以外からの不正な振込依頼を無くすことができ、これによってセキュリティを確保することができるとともに、振込依頼者以外の第３者に振込内容が知られないようにして、プライバシーを確保することができる。

【００３６】《第１の実施の形態の変形例》なお、この実施の形態においては、電子振込制御装置３０側では、通信回線網４０を介して電話が受けられると、通信回線網４０から通知される発呼元の電話番号が、既に振込許可を出している振込依頼者（振込データ用暗号化キーを通知してある申込者）側の電話番号かどうかが振込依頼者チェック部３２によりチェックするように構成したが、これは、オペレータ自身がチェックするようにしても良い。この場合、オペレータは、発呼元の電話番号が既に振込許可を出している振込依頼者側の電話番号でなければ、不正なアクセスであると判断して、通信回線を切断する（ステップＳＴ８、ＳＴ９）。一方、オペレータのチェックの結果、発呼元の電話番号が既に振込許可を出している振込依頼者側の電話番号であれば、電子振込制御装置３０によって発呼元の電子振込端末装置２０との間の通信回線を確立するとともに、送信許可応答を通信回線網４０を介して、電子振込端末装置２０に送信する（ステップＳＴ８）。

【００３７】また、この実施の形態においては、照合部２８を設けて、送信データと受信データとの照合一致を確認するように構成したが、この照合部２８を省略し、送信データと受信データとの照合一致は、振込依頼者自身がチェックするようにしても良い。チェックの結果、送信した振込データと相違する場合、あるいはチェック結果に不満があるときには（前述したステップＳＴ２３）、振込キャンセル通知が作成され、これが金融機関側の電子振込制御装置３０に送信されて、振込処理がキャンセルされた後、通信回線が切断される（前述したステップＳＴ２４、ＳＴ２５）。一方、自分が送信した振込データの内容と、金融機関側から送信されてきた振込データの内容とが合致し、チェック結果が満足するものであるときには（ステップＳＴ２３）、振込データの送信が正しく行われているので、電子振込端末装置２０を操作して振込指示通知を作成し、これが金融機関側の電子振込制御装置３０に送信される。そして、振込処理が実施された後、通信回線が切断される（ステップＳＴ２６、ＳＴ２７）。

【００３８】《第２の実施の形態》上述した第１の実施の形態においては、通信回線網４０を使用して、電子振込端末装置２０で作成された振込データを電子振込制御装置３０に通知するようにしているが、通信回線網４０による通信以外の方法、例えばＩＣカードの授受により、電子振込端末装置２０で作成された振込データを電子振込制御装置３０に通知するようにしても良い。

【００３９】この場合、図７に示すように、申込者が金融機関側に申込書を提出した時点で、申込者に振込データ用暗号化キーと、ＩＣカードとが渡される。この申込者（振込依頼者）は、振込依頼を行うとき、前記振込データ用暗号化キーを使用して、振込データを暗号化してＩＣカードに記憶させる。このＩＣカードが金融機関側の窓口に提出されると、このとき振込依頼者に対して照会番号が教えられる。

【００４０】次いで、金融機関側では、前記振込依頼者に通知している振込データ用暗号化キーに対応する振込データ用復号化キーを使用して、ＩＣカードに記憶されている暗号化された振込データを復号化する。そして、復号された振込データの内容に基づき、振込を許可するかどうかを判定する。

【００４１】この後、振込依頼者によって金融機関側に電話がかけられ、金融機関側の担当者に前記照会番号が通知され、この照会番号が正規の照会番号であると判定されたとき、振込依頼者に前記判定結果が通知され、この通知内容に基づき、前記振込依頼者によって、金融機

関側に振込指示通知、振込キャンセル通知が行われるのである。

【００４２】このようにしても、上述した第１の実施の形態と同様に、事前に申し込んだ振込依頼者以外からの不正な振込依頼を無くすことができ、これによってセキュリティを確保することができるとともに、振込依頼者以外の第３者に振込内容が知られないようにして、プライバシーを確保することができる。

【００４３】さらに、第２の実施の形態では、通信回線網４０を使用していないことから、通信回線網４０上での情報漏れなどが発生しないようにすることができ、これによって情報漏れに起因する第３者の不正アクセス、不正振込などを完全に防止することができる。

【００４４】

【発明の効果】以上説明したように本発明によれば、請求項１、３では、通信回線を介して、振込の依頼を行う際、事前に申し込んだ振込依頼者以外からの不正な振込依頼を無くすことができ、これによってセキュリティを確保することができるとともに、振込依頼者以外の第３者に振込内容が知られないようにして、プライバシーを確保することができる。

【００４５】また、請求項２では、ＩＣカードを使用して、振込の依頼を行う際、事前に申し込んだ振込依頼者以外からの不正な振込依頼を無くすことができ、これによってセキュリティを確保することができるとともに、振込依頼者以外の第３者に振込内容が知られないようにして、プライバシーを確保することができる。

【図面の簡単な説明】

【図１】本発明に係る電子振込システムの実施の形態を示すブロック図である。

【図２】図１に示す電子振込システムにおける事前審査手続き時の動作例を示すフローチャートである。

【図３】図１に示す電子振込システムにおける振込依頼手続き時の動作例を示すフローチャートである。

【図４】図１に示す電子振込システムにおける振込依頼手続き時の動作例を示すフローチャートである。

【図５】図１に示す電子振込システムにおける振込依頼確認手続き時の動作例を示すフローチャートである。

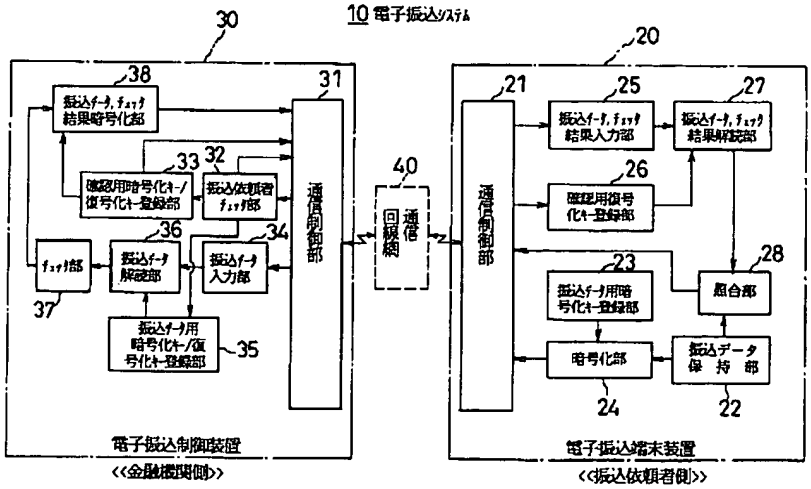
【図６】図１に示す電子振込システムにおける振込依頼確認手続き時の動作例を示すフローチャートである。

【図７】本発明に係る電子振込システムの他の実施の形態を示すフローチャートである。

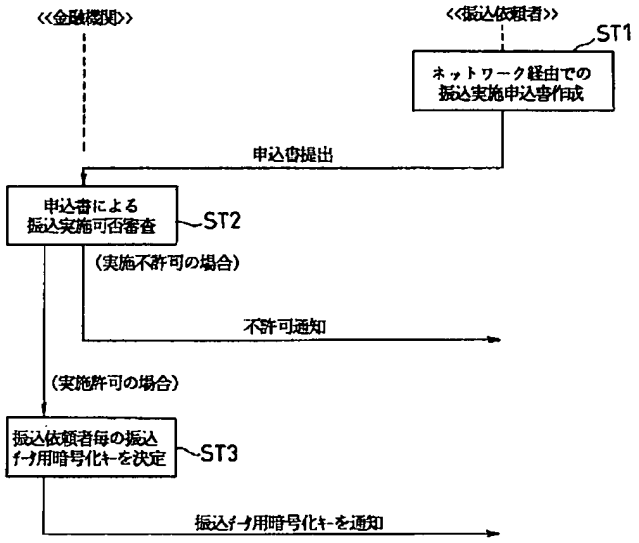
【符号の説明】

１０　電子振込システム
２０　電子振込端末装置
２１　通信制御部
２２　振込データ保持部
２３　振込データ用暗号化キー登録部
２４　暗号化部
２５　振込データ、チェック結果入力部
２６　確認用復号化キー登録部
２７　振込データ、チェック結果解読部
２８　照合部
３０　電子振込制御装置
３１　通信制御部
３２　振込依頼者チェック部
３３　確認用暗号化キー／復号化キー登録部
３４　振込データ入力部
３５　振込データ用暗号化キー／復号化キー登録部
３６　振込データ解読部
３７　チェック部
３８　振込データ、チェック結果暗号化部
４０　通信回線網

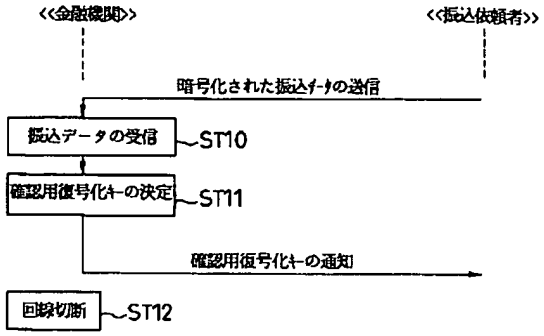
【図１】



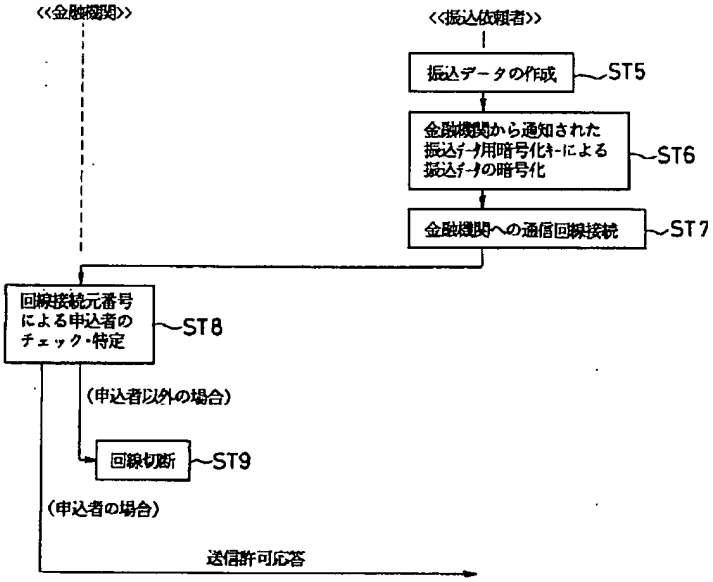
【図２】


<<金融機関>>
<<振込依頼者>>
ST1
ネットワーク経由での振込実施申込書作成
申込書提出
申込書による振込実施可否審査
ST2
(実施不許可の場合)
不許可通知
(実施許可の場合)
振込依頼者毎の振込データ用暗号化キーを決定
ST3
振込データ用暗号化キーを通知

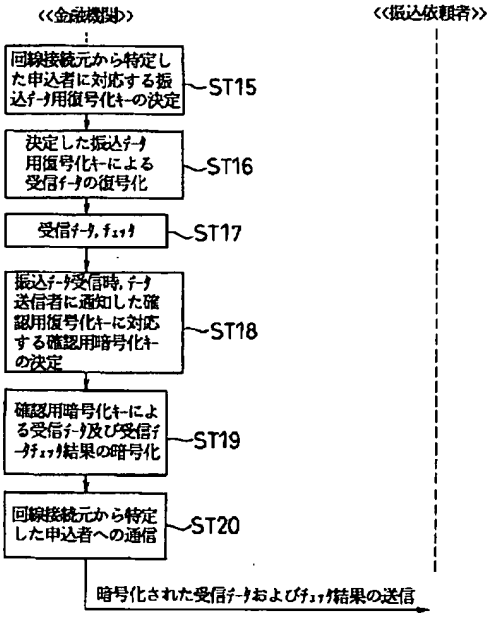
【図４】


<<金融機関>>
<<振込依頼者>>
暗号化された振込データの送信
振込データの受信
ST10
確認用復号化キーの決定
ST11
確認用復号化キーの通知
回線切断
ST12

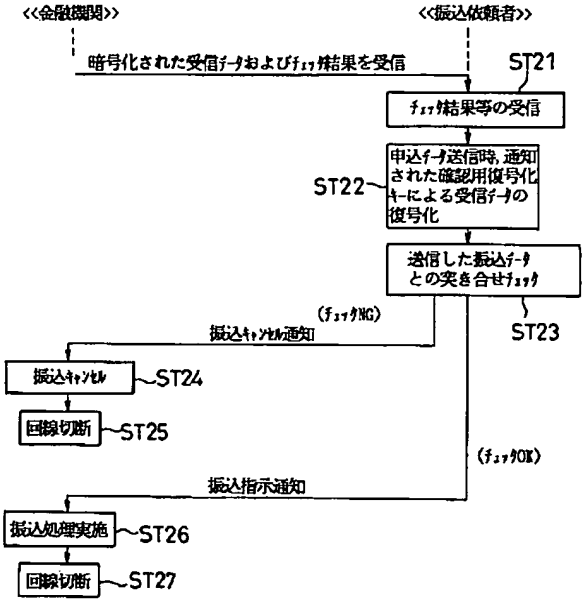
【図３】


<<金融機関>>
<<振込依頼者>>
振込データの作成
ST5
金融機関から通知された振込データ用暗号化キーによる振込データの暗号化
ST6
金融機関への通信回線接続
ST7
回線接続元番号による申込者のチェック・特定
ST8
(申込者以外の場合)
回線切断
ST9
(申込者の場合)
送信許可応答

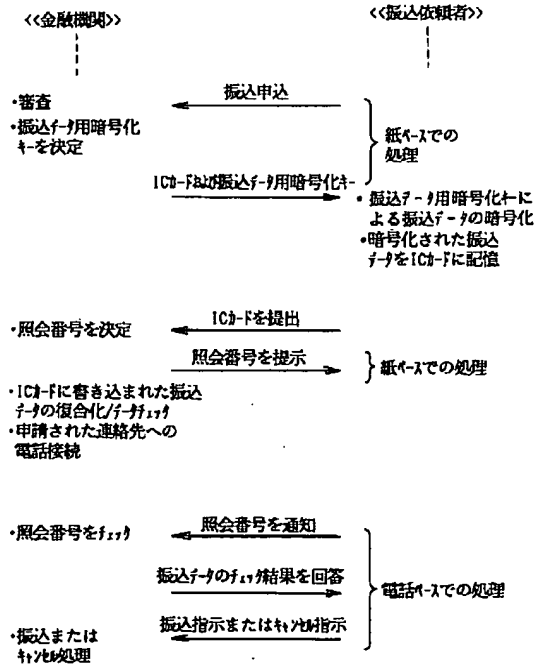
【図５】


<<金融機関>>
<<振込依頼者>>
回線接続元から特定した申込者に対応する振込データ用復号化キーの決定
ST15
決定した振込データ用復号化キーによる受信データの復号化
ST16
受信データ，チェック
ST17
振込データ受信時，データ送信者に通知した確認用復号化キーに対応する確認用暗号化キーの決定
ST18
確認用暗号化キーによる受信データ及び受信データチェック結果の暗号化
ST19
回線接続元から特定した申込者への通信
ST20
暗号化された受信データおよびチェック結果の送信

【図６】


<<金融機関>>
<<振込依頼者>>
暗号化された受信データおよびチェック結果を受信
ST21
チェック結果等の受信
申込データ送信時，通知された確認用復号化キーによる受信データの復号化
ST22
送信した振込データとの突き合せチェック
ST23
(チェックNG)
振込キャンセル通知
振込キャンセル
ST24
回線切断
ST25
(チェックOK)
振込指示通知
振込処理実施
ST26
回線切断
ST27

【図７】


<<金融機関>>
<<振込依頼者>>
・審査
・振込データ用暗号化キーを決定
振込申込
紙ベースでの処理
ICカードおよび振込データ用暗号化キー
・振込データ用暗号化キーによる振込データの暗号化
・暗号化された振込データをICカードに記憶
・照会番号を決定
ICカードを提出
照会番号を提示
紙ベースでの処理
・ICカードに書き込まれた振込データの復合化/データチェック
・申請された連絡先への電話接続
・照会番号をチェック
照会番号を通知
振込データのチェック結果を回答
振込指示またはキャンセル指示
電話ベースでの処理
・振込またはキャンセル処理